View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Theseus

LAUREA
UNIVERSITY OF APPLIED SCIENCES
Together we are stronger

Ethical and societal analysis on data protection, privacy, security and freedom of victims in USAR: A literature review

Thapa, Megha
Oke Folawunmi Olasunkanmi

2015 Leppävaara

Laurea University of Applied Sciences
Leppävaara

Ethical and societal analysis on data protection, privacy, security and freedom of victims in USAR: A literature review

Megha Thapa
Oke Folawunmi Olasunkanmi
Degree Programme in BIT
Bachelor's Thesis
May, 2015

Laurea University of Applied Sciences
Leppävaara
Business Information Technology

Abstract

Thapa, Megha; Oke Folawunmi Olasunkanmi

Ethical and societal analysis on data protection, privacy, security and freedom of victims in USAR: A literature review

Year 2015 Pages 32

Disasters occur, whether man-made or natural and Urban Search and Rescue (USAR) task-forces are responsible for the safe rescue of people. In the rescue operations, gathering and transforming data from the beginning of the operation till the end are important in other to use accurate information in rescuing victims.

The aim of this study includes investigating the ethical and societal issues related to data protection, privacy and security and freedom in USAR operations. In addition, it explores the available standards, best practices and legal issues considerations for data protection, privacy and security. Furthermore, it aims at providing high-level conceptual framework for better processes of data protection, privacy and security and freedom in USAR operations.

A literature review process was used during this study. The search for articles related to the subject matter was carried out using the Nelli database and various literatures which would promote the aim of this review were found. Using a set inclusion and exclusion criteria, the relevant articles were filtered and the needed information was extracted.

This review revealed that search and rescue missions are evolving with the introduction of technology alongside human effort. Various forms of technology are being developed to assist in saving the lives of victims and the processes involved in securing the information of these victims are not given enough attention. Also, recommendations for further studies are stated based on the research findings.

Keywords: Urban search and rescue, data protection, privacy

Table of contents

1 Introduction 6
1.1 Background information 6
1.2 Objectives of the study 7
1.3 Research questions 7
2 Theoretical background 7
2.1 Urban search and rescue (USAR) 7
2.2 Data protection 8
2.3 Privacy 8
2.4 Security and freedom of victims 9
2.5 Common issues with data protection and privacy 9
2.5.1 Abuse of administrative rights 9
2.5.2 Human error 10
2.5.3 Lack of proper training 10
2.5.4 Inappropriate handling of passwords 11
2.5.5 Threat by hackers 11
2.5.6 Negligent destruction of data 12
2.5.7 Improper use of data 13
2.5.8 Leakage of data 13
2.5.9 Inadequate privacy protection 14
2.6 Solutions to common issues with data protection and privacy 15
2.6.1 Proper security training and awareness program 15
2.6.2 Appropriate access control rights defined 16
2.6.3 Data destruction plan 16
2.6.4 Proper background check of users 17
2.6.5 Security of software interface 17
2.6.6 Guidelines to regulate the data 17
2.6.7 Controlling facilities and physical access 18
2.6.8 Managing Personally Identifiable information properly 18
3 Research method 19
3.1 Data collection 19
3.2 Data analysis 20
4 Findings 22
4.1 Urban search and rescue (USAR) 22
4.2 Data protection and privacy 23
5 Discussion 24
5.1 Reliability and trustworthiness 26
5.2 Project work and learning reflection 26
5.3 Conclusion 27

5.4 Recommendations 27
References 28
Figures 31
Tables 32

1 Introduction

Natural and man-made disaster occurs that turns normal day-to-day life and situation into challenging one. Many times, people get trapped inside collapsed building or in the midst of unsafe circumstances - either dead or with little chance of survival. Urban Search and Rescue (USAR) task forces are responsible for safely rescue of people. For example, USaR are tasked with the job of searching for survivals within the rubbles of the collapsed structures with the use of various tools at their disposal, gather information and take the optimum course of action to ensure safe recovery of the victims. In the rescue operations, gathering and transforming data from the beginning of the operation till the end are very important. All data acquired should be kept confidential due to its delicate nature. The information should only be accessible by the right group of people involved in the rescue operation, privacy of everyone involved should be prioritized. Data storage, processing and disposable should be done securely. Hence, information security and assurance plays extremely important role in search and rescue services.

1.1 Background information

INACHUS is an acronym which stands for Technological and Methodological Solutions for Integrated Wide Area Situation Awareness and Survivor Localization to Support Search and Rescue Teams. INACHUS is a project aiming at providing an integrated platform in urban search and rescue operations to assist the operations of first responders and USAR teams. This is an European commission project which aims at achieving time reduction and increased efficiency in urban search and rescue operations that will enhance the operational effectiveness of people involved in challenging USAR and first response activities.

INACHUS aims to achieve a significant time reduction related to Urban Search and Rescue (USAR) phase by providing wide-area situation awareness solutions for improved detection and localization of the trapped victims assisted by simulation tools for predicting structural failures and a holistic decision support mechanism incorporating operational procedures and re-sources of relevant actors. One part of the INACHUS project which will be the focus of this review is the INACHUS ethics project.

The main objective of this INACHUS ethics project is to secure that ethical and societal issues will be taken into account in the technical system, user guidelines as well as in the business model of the solution and aims to promote ethical and societal justice and acceptability of the INACHUS solution.

1.2 Objectives of the study

The objectives of this research include but are not limited to:

- Investigating the ethical and societal issues related to data protection, privacy and security and freedom in USAR operations.
- Exploring the available standards, best practices and legal issues considerations for data protection, privacy and security.
- Providing high-level conceptual framework for better processes of data protection, privacy and security and freedom in USAR operations.

1.3 Research questions

The research questions are:

- What information of victims is available publicly and privately to USAR?
- How does USAR gather and use the information about disaster victims?
- How does USAR secure the data collected before, during and after the disaster?
- What data protection mechanism are considered and implemented by USAR?
- How does USAR respect and protect the privacy of victims?
- How is security and freedom of victims considered and implemented by USAR?

Literature search will be done to find published articles/subjects relating to urban search and rescue, data protection, privacy and security and freedom of victims. The analysis of the result of this search will be pivotal in answering these questions.

2 Theoretical background

2.1 Urban search and rescue (USAR)

The process of locating, extricating, and providing on-scene medical treatment to victims trapped as a result of natural and artificial disasters is USAR (Hew & Sunshine 2002). “Urban search-and-rescue is considered a "multi-hazard" discipline, as it may be needed for a variety of emergencies or disasters, including earthquakes, hurricanes, typhoons, storms and tornadoes, floods, dam failures, technological accidents, terrorist activities, and hazardous materials releases” (Federal Emergency Management Agency 2014).

Each USAR task force is highly-trained, multi-disciplinary organization that perform physical, electronic and canine search. Their tasks includes extricating victims from collapsed structures, providing emergency medical cares to victims and rescuers, assess and control the affected utilities, perform hazardous material monitoring; and evaluate and stabilize damaged

structures. Each task force strives to have highly trained technical specialists that include law enforcement officers, physicians, structural engineers, hazardous material technicians, heavy rigging specialists, firefighters, paramedics and canine handlers. Each task force has an equipment cache to support disaster operations. The cache includes construction-type tools, electronic equipment, medical supplies, hazardous material monitoring equipment, protective gear, communications equipment, computers, video and photographic recording devices, administrative supplies, materials to feed, shelters and support the task force. USAR task forces are equipped to respond any type of disaster including man-caused intentional and accidental events and natural disasters. (Wong & Robinson 2004)

2.2 Data protection

The data protection controls how personal information is used by organizations or by government bodies. According to the EU data protective directive “"personal data" shall mean any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity” (Data protection commissioner 2007).

According to the IT-Grundschutz (2005), the duty of data protection is to protect the individual so that one is not disadvantaged in their personal rights through the handling of their personal data. Data protection contains all the actions that are used for storing, backup, restoring and destroying the data. The basis for data protection is confidentiality; the unauthorized collection, processing and storage of personal data by individual involved in processing personal data are prohibited.

2.3 Privacy

Privacy is a fundamental human right and is perhaps considered to have different definitions. Definitions of privacy vary widely according to the context and environment. It has been defined in different ways by a variety of authors and institutions. The authors Warren and Brandies had defined privacy as the right to be alone and is the first definition of privacy given in year 1890 (Kotler 2009, 21).

According to the universal declaration of human rights (2015), right to privacy states that “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks” (The Universal Declaration of Human Rights 2015).

Roger Clarke (2013) defines privacy as the interest that individuals have in sustaining a 'personal space', free from interference by other people and organizations.
Privacy is an outcome of a person wish to withhold from others certain knowledge as to his past and present experience and actions and his intentions for future. The threats to privacy come from sources such as technology, government and cooperation.

2.4 Security and freedom of victims

Victims of disaster should be located and rescued from the trapped situation. The victims under the rubbles should be detected and that increases the chance of rescue and survival. The first responder should locate the survivor of the disaster and target on saving them. The survivors of such situations should be informed and consulted on measures to be taken and procedures to be followed. (IASC operational guidelines on the protection of persons in situations of natural disaster 2011)

The security of the victims should be ensured and once the victims are rescued they should be moved to the more secured place. The affected persons should be protected and not exposed to the further risk. They should be provided immediate medical treatment and informed about the potential secondary impacts. (IASC operational guidelines on the protection of persons in situations of natural disaster 2011)

2.5 Common issues with data protection and privacy

2.5.1 Abuse of administrative rights

Abuse of administration rights occurs when the super user privileges acquired either rightfully or illicitly, are deliberately used to harm the system or its user .The access right to data, information should be given to limited people to ensure the secure and proper use of IT systems and processes. If such rights are granted to the wrong person, or if a right is abused, this can give rise to a variety of threats which can compromise the confidentiality and integrity of data. (Horwath 2012)

One of the principles of security is least privilege. Least privilege should be applied limiting each authorized individual’s access to the minimum information and resources to perform their legitimate duties and functions. When someone is granted privileges that exceed the requirements of their job function, these privileges can be abused. Many times users receive group privilege with the purpose of one-size fits all. Granting the right amount of privilege and being able to detect excessive privileges can be time consuming, but will help increase the security posture of an organization. (Horwath 2012)

In some cases, users abuse the privileges for unauthorized purposes. Users in position of authority with privilege can abuse their authority for unauthorized access to data, or perform actions beyond their job duties. The access rights should be given according to the user role, task and position. The users that have excessive rights that are not required to do their job should be identified and removed. (Horwath 2012)

2.5.2 Human error

Human error ranges from accidental deletion of files and records to ignoring policies regarding data to rebooting systems without proper shutdown procedures. Users often make mistakes, and as a result data is lost. The major human error is the failure to follow procedures and to stay within the operational envelope. (Janes 2012)

Users intentionally or unintentionally send sensitive email to the wrong email address, or certain information being disclosed by mistake in response to a request. The users may misplace or lose laptops, USB drives, smart phones, print outs, or backup tapes with proprietary or protected data while travelling or within the office. Data stored can fall into unauthorized hands. (Janes 2012)

Blind belief and trust in fellow workers and leaving the information open to the fellow workers happens often in working life. This gives unauthorized members of staff access to protected files or confidential information. Due to the carelessness of the users, data can be lost or stolen. The sensitive data are disposed inadequately, due to which a wrong person can get access to this data.

The users with access to sensitive data may intentionally or unintentionally delete the information. Due to incorrect administration of access rights, an employee can be able to modify data without realizing the critical impact of such a violation of integrity. (IT-Grundschutz 2005)

One of the example of human error according to IT- Grundschutz 2005, is employees often communicate confidential information about the critical situation over mobile phones on trains or in restaurants. This information is not only heard by the person the other end but also by everyone around.

2.5.3 Lack of proper training

The users receive inadequate training in the operation of the technologies that they use. This may result in serious security problems due to unintentional, incorrect use, wrong configura-

tion and inappropriate equipment. Individual training in Information Security is mandatory, any technical training appropriate to the user's job function should be provided. Where user change jobs, their Information Security needs must be re-assessed and new training provided if needed. (IT-Grundschutz 2005).

One of the example of lack of proper training according to IT- Grundschutz 2005, is employees get attacked with techniques that result in stolen access credentials. Because of lack of proper training, users are unable to figure out those problems and are easy prey for attacks.

2.5.4 Inappropriate handling of passwords

The use of authentication procedures will be little advantage if the users are careless in handling the access-granting means. The passwords, tokens, pin codes are some of the examples of the access-granting means. These are often disclosed to other persons or coworkers for reason of convenience or as a friendly gesture. Passwords are frequently shared within team so that it is easier for individual staff to access shared files. Not every team members may have equal access rights and sharing passwords gives a user with less access right, access to the excessive amount of data and one can use it to harm the system. The users disregard the security issues for their comfort and flexibility. (IT-Grundschutz 2005).

When large numbers of passwords are used, users often cannot remember them all. To prevent their password to be forgotten, users usually write down the passwords. Passwords are not changed frequently and users choose simple passwords. These are not considered as problems as long as they are carefully looked after, so that they are protected against unauthorized access. Some users overlook the security aspects for example, the passwords are written down and placed underneath the keyboard, and stickers are attached to the screen. (IT-Grundschutz 2005).

Where a token-based procedure (e.g. smart card or one-time password generator) is used for user authentication, if this is lost there is a danger that the token could be used by unauthorized persons. The loss of passwords or tokens can even result in loss of user data. An unauthorized user might be able to access all the data that contains the information about the survivors. (IT-Grundschutz 2005).

2.5.5 Threat by hackers

Hackers are those individuals who carry out attacks on computer systems or networks in order to gain access illegally. Different techniques are used to penetrate a network which could be for fun or for a specific reason and this is done persistently until the desired result is

achieved. After a successful penetration, malware could be installed onto the system to steal private information and also Trojans which create a back door on the system for the hacker in case attacker wishes to return to cause more damage (Britz 2013; Webroot 2014).

Hackers may steal usernames and/or passwords or grant unto themselves administrative rights to a system in order to gain easy access. Information such as names and social security numbers can be stolen and sold to other parties who will use them for destructive purposes (IT-Grundschutz 2005).

Wireless networks such as Bluetooth and wireless LANs can also be breached by hackers. Bluetooth devices can be used for transmission between various technologies and frequencies using this medium can travel for up to 100 meters. Devices which transmit using Bluetooth have been found to be vulnerable to attacks such as bluejacking, bluescanner and bluesnarfing. Bluejacking refers to when a Bluetooth user receives unwanted or unnecessary information. Bluescanner refers to a program which forces itself into other Bluetooth devices and gathers information off them. Bluesnarfing refers to when data is stolen from a user. (Gregg 2013)

Wireless LANs are commonly used when referring to wireless security at the moment. Unlike the Bluetooth, it is not as easy to penetrate and data is transmitted using electromagnetic waves as well as covering a larger area of space. However, wireless LANs has its own vulnerabilities such as eavesdropping, denial of service and open authentication. (Gregg 2013)

Eavesdropping can happen when an attacker intercepts the transmitted signals over a network and decodes the information. The attacker could be located nearby or further away and intercept using and antenna. (Gregg 2013)

Denial of service happens when then the attacker targets part of or the whole system and render it difficult to use or unusable. (Gregg 2013)

Open authentication occurs when a network authentication is left open and attackers have access freely and unchallenged. An IP address in the network may be used for malicious purposes by the attacker which will be traced back to the owner of the network and not the attacker. (Gregg 2013)

2.5.6 Negligent destruction of data

Thoughtless usage of the delete command can erase completely the file arrangements. Negligence and inexperienced usage could lead to the damage of equipment or information which can brutally disturb continuous operation of the IT system. An example can be spilling coffee

or any drink which can cause humidity and allow for short-circuit problem in the IT system (IT-Grundschutz 2005).

When data is collected manually and converted into electronic format, the destruction process of the hard copy should not be ignored. Dumping of such documents in the trash bin is not enough to complete a destruction process (Archives Management Centers, Inc. 2014). Also, pressing the delete key on the keyboard of a computer does not necessarily mean that the data has been erased from the system. It is still possible for these data to be recovered by those who are determined to do so (West Coast Computer Recycler 2013).

2.5.7 Improper use of data

Data collected for life rescuing process are meant to be analyzed and used for the appropriate reason. It should not be manipulated or altered for personal reasons or sold to third parties for financial gains. Unnecessary copies of sensitive data should not be made, should be used only during the time frame it is needed and destroyed immediately it outdates its usefulness (IT-Grundschutz 2005).
Unauthorized personnel should not have access to the database management system; otherwise, they could take or use any data for their own personal reasons (IT-Grundschutz 2005).

2.5.8 Leakage of data

Confidentiality is an important aspect of security and can be breached due to errors on the part of IT users. Personal information gathered about the lives of people involved during the rescue operation should not be made available unnecessarily or left out in the open for those without the appropriate access rights to view or tamper with such information. Leakage can also occur during the gathering phase of data through an insecure manner in which data is transported or moved around from one location to the other (IT-Grundschutz 2005).

Information should be protected and put in a secured location where only authorized personnel have access. Private information should not be stored on the local server where everyone can have access and duplicated as needed. An attacker could infiltrate such unsecured servers and take any information and use for malicious purposes. Also, information should be checked and verified before actions are taken or the information sent to appropriate quarters (IT-Grundschutz 2005).

Incorrect access rights can also allow data to be modified, mixed up or moved without knowing its full impact or out of curiosity. Information can also be leaked unknowingly if the user

has little knowledge about the IT system or is negligent enough to leave the computer unlocked while away (IT-Grundschutz 2005).

Confidentiality attacks can include packet sniffing and session hijacking which is perpetrated by an attacker. Packet sniffing occurs as a result of eavesdropping on transmissions within a local area network. When an attacker finds a way unto a network, he uses sniffing software to listen in on the network for user names and passwords which are not encrypted. Session hijacking on the other hand, the attacker acquires the session cookies and continues to operate as the user without any suspicion. (Sloan & Warner 2013)

2.5.9 Inadequate privacy protection

When personal information about victims are left unprotected or secured using light security measures such as easy to guess passwords or no password at all, it is easy for the privacy of victims to be breached. Ineffective encryption methods in securing sensitive data will allow for easy access by attackers to crack open such data, steal or manipulate it for their own gains (Datashield 2013).

Storing of sensitive information together with other general information increases the risk of exposure and further jeopardizes the privacy protection of victims. All Information stored should be categorized based on its importance and then secured in the same manner.

Figure 1: Common issues with data protection and privacy

2.6 Solutions to common issues with data protection and privacy

2.6.1 Proper security training and awareness program

According to IT-Grundschutz, IT training should cover a number of areas such as staff-related IT safeguards, product-related IT safeguards, procedures in case of computer virus infection, the importance of data backup and its implementation, handling personal data, briefing on emergency measures, prevention of social engineering and building IT security awareness (IT-Grundschutz 2005, 1661).

Staff-related IT safeguards handle everything personnel related and how the staff should act in their daily work routines. Product-related IT safeguards covers how to use supplied software correctly. Building IT security awareness attempts to make the staff aware of how important IT security is to the organization and how their effort is what makes the difference between the system being secure or unsecure.

Below are the most important steps in creating a training and awareness program according to the IT-Grundschutz.

To create an organized training program, the objectives of the program must be clear. The organization needs to know what they wish to change in the staffs actions. This also helps to measure the success of the training program afterwards.

Different staff member groups need different IT skills and thus, need different training. The different staff groups could be: management, administrators, IT staffs, other staffs and more if needed. The amount of IT system and software training varies greatly between the different groups. Administrators' and IT staff's training requirements are not the same as an accountant's training (IT-Grundschutz 2005, 1574).

All staff members should familiarize themselves with the relevant safeguards of their working environment. Therefore it is important that there isn't an overwhelming amount of rules and regulations concerning IT safeguards. As we mentioned before IT security must not be seen as a hindrance of the workflow. This ties in well with proper training, as properly trained staffs are accustomed to following the safeguards automatically. To promote this behavior the IT security training should be done simultaneously with the organizations other training (IT-Grundschutz 2005, 1576).

As IT keeps rapidly developing, new IT systems and software as well as new threats appear. The training must keep up with the constant changes. The training program itself must be updated regularly and the staff members themselves need new training as well.

The security training can be done by the organizations own staff members or outsourced to experts. Both options have their own benefits and drawbacks. If the organization's own staff members are used for the training, they are drawn away from their other tasks. They also must be skilled in the subject they are teaching and willing to spread the knowledge they have (IT-Grundschutz 2005, 1779). The trainers must also be confident in their communication skills.

2.6.2 Appropriate access control rights defined

Only authorized individuals should be allowed into workplaces which contain sensitive information. Passage can be regulated through access cards being distributed to employees, or a manual checkpoint at the building entrance. Implementing such a control will greatly reduce the risk of deliberate acts being caused.

Doors inside the building which lead to rooms containing sensitive information should always be locked, and access through them should only be permitted to certain individuals. For example, access to a server room should only be permitted to the server administrators, or to cleaning personnel who are either supervised or have been given the right training and instructions. The access control can be set in place by installing biometric or keycard scanners and key locks. This can ensure that confidential or top secret information won't end up in the wrong hands. Same procedures should be implemented for cabinets and drawers (IT-Grundschutz 2005, 727/730).

2.6.3 Data destruction plan

It is important to ensure the privacy and security of victims by destroying data collected during the disaster after the whole operation has ended. Consent should be sought from the victim or victim's family if the data would be needed for an extended period. People involved should be notified about what information is needed and what the information will be used for before asking for their consent. Consent should be given freely and should not be made compulsory or received under duress (Sloan & Warner, 2013). Consent can also be withdrawn at any time by the concerned individual. (Handbook on European data protection law, 2014)

Destroying data after it is no longer needed should be done properly and ensure it leaves no trace upon which information can be retrieved. Physical destruction of data can occur in dif-

ferent ways, for example, shredding or melting in order to make data unreadable or inaccessible to unauthorized personnel. Another way of destroying data is through overwriting old data with new data. This way, normal data can be saved over the sensitive data a number of times to ensure it leaves no trace. Encryption the data and destroying the encryption key along with such data also ensures its security. Also, degaussing is another effective way of data destruction. It involves the use of a magnetic field to destroy the magnetic fields on the storage device. When degaussing is applied, it leaves no trace which is best for sensitive data. (Stutzman; Violino, 2012)

2.6.4 Proper background check of users

Proper checks should be carried out before hiring personnel who will see to the daily usage of collected data. These checks will make known information as to whether hired personnel can be trusted with private information without the fear of misusing such information and privacy laws being breached. Criminal records, educational credentials should be checked and family relations considered as well. For example, the Fair Credit Reporting Act (FCRA) is a standard to be followed in carrying out background checks of employees in the United States of America.

Also, where additional or increased access rights is to be given to a staff, extra background checks should be done to confirm if the staff could be entrusted with such a sensitive position. Every detail about the staff's routine and actions should be examined.

2.6.5 Security of software interface

With the increased use of computer-based information systems, there has been a rise in calls for concern regarding the protection of computer-processed data. A strong security of interface used ensures the security of computer-processed data from unauthorized access, from destructive user actions, and from computer failure. (IT-Grundschutz 2005).

2.6.6 Guidelines to regulate the data

IT users should be instructed on how to store, handle and protect data in a clear, well-structured manner. Poorly regulated data may lead to a variety of problems (IT-Grundschutz 2005, 1084). Proper set of guidelines should be implemented to avoid the leakage of data and these rules must be conveyed to all the employees. While creating guidelines, it is important to take legal, governmental, human rights in consideration.

A clear documentation explaining the rules and regulations to regulate data should be created that help users to understand the goal of the document. Due to rapid changes in the IT operating and security environment, policies, standards and procedures should be regularly reviewed and updated to make sure that the policies adequately protect confidential information. It should also be effectively communicated to employees. (Data Protection and Breach Readiness Guide 2014)

2.6.7 Controlling facilities and physical access

Limiting access to the data center and its boundary is one of the most effective means for limiting the damage from a malicious act, which would potentially result in a privacy incident, is to limit access to the data center and its boundary, including data center and the adjacent areas. This is often either ignored or overlooked. (Herold 2006)

The sensitive areas of information processing facilities should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. Access rights should be restricted as much as possible to ensure that unauthorized persons cannot enter the areas and access personally identifiable information (PII). (Herold 2006)

The implementation of procedures to control and validate a person's access to facilities based on their role or function, including visitor control is required. This will limit the access to sensitive areas to authorized personnel only. Access to the sensitive areas can be controlled by password, token, badge system or card reader mechanisms for entry points. (Physical and environmental security 2008)

2.6.8 Managing Personally Identifiable information properly

The rescue team often needs access to information about all the people influenced by the disasters. It includes broad range of information that can identify individuals, including home address, date of birth, contact information and many others. These personally identifiable information (PII) needs to be protected. (NIST 2010)

These PII should be protected through combination of measures, such as operational safeguards, privacy specific safeguards, security controls. Organization should develop policies and procedures for handling PII at the organization level, program level and if possible also at the system level. Various factors should be considered while developing privacy policies such as access rule for PII within a system, PII retention schedules and procedures, PII incident response and data breach notification, limitation of collection, disclosure, sharing and use of PII and consequences for failure to follow privacy rules behavior. Activities like awareness, train-

ing and education are crucial to the success of privacy. The data should be collected, maintained, used and distributed in such a way that protects the confidentiality of data. The irrelevant PII should be properly destroyed. (NIST 2010, 24)

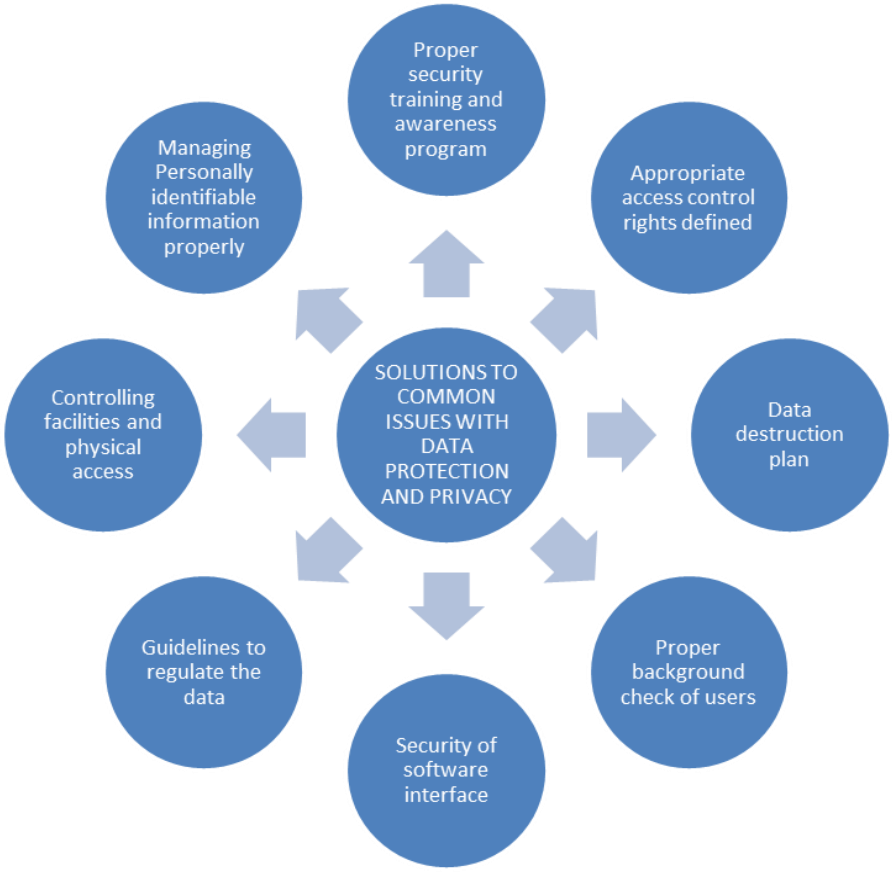

Figure 2: Solutions to common issues with data protection and privacy

3 Research method

The method used in this research is the systematic review. This method aims to identify and analyze literature according to a set criteria or keywords deduced from the research questions. Investigation will be carried out about studies related to the questions being researched. Literature to be considered will be articles from databases within Nelli relating to urban search and rescue, data protection, privacy, security and freedom. Using Nelli databases, investigation was carried out on the data protection, privacy and security and freedom of USAR operations.

3.1 Data collection

Databases used in conducting this research include Academic Search Elite (EBSCO) and CINAHL (EBSCO). The search for sources or material was conducted on the 10th of December 2014.

Table 1 shows the combination of terms used in this search which include “Urban search and rescue”, “data protection” or privacy*, security* and freedom*, “Urban search and rescue” and freedom* and “Urban search and rescue” and privacy*. **Error! Reference source not found.**below also shows the combined result totaled to 64,925 articles and further reduced to 28,699 when we considered only full text articles.

Database	*“Urban search and rescue”*	*“Data protection” OR Privacy**	*Security* and Freedom**	*“Urban search and rescue” and freedom**	*“Urban search and rescue” and privacy**
Academic Search Elite (EBSCO)	127	40,851	9,142	3	0
CINAHL (EBSCO)	11	14,680	114	0	0
Total	138	55,531	9,256	3	0

Table 1: depicts the literature search results and the categorized number of hits using five different keywords.

Inclusion criteria	Exclusion Criteria
Articles in full text and free	Articles not in full text
Articles relevant to the research	Articles not relevant to the research
Articles in English	Articles not in English

Table 2: This table shows the inclusion and exclusion criteria.

3.2 Data analysis

Table 2 shows that the inclusion criteria were based on studies and/or articles in full text, in English and relevant to the research. After excluding all results not in full text, the articles with full and free text was then streamlined after considering titles, abstracts and relevance to 14 articles. The articles to be thoroughly analyzed had to contain areas of urban search and rescue, data protection or privacy and freedom of victims which were relevant to this study. These articles chosen were read in detail analyzed and downsized to 7 which were most relevant to the study (Figure 3: second and third steps) and these articles were published between 2002 and 2014. These articles were analyzed based on the significance of their contents with relevance to the subject. The fourth step (Figure 3) entails the interpretation of findings.

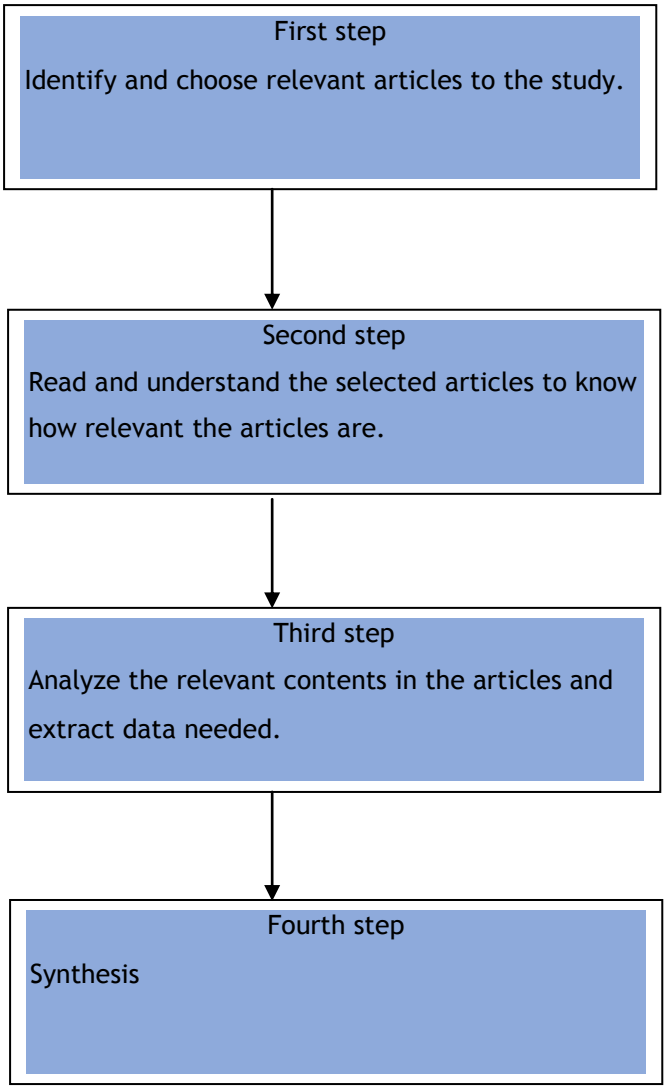

Figure 3: The literature review process.

4 Findings

USAR uses technologies like mobile phones, snake robots, sensors, satellites etc. to locate survivors inside the collapsed building, gather information within the environment and rescue victims trapped in such situation. With the increasing use of technologies in such situation comes a growing need to identify the ethical consequences that befall such technologies in order to ensure the privacy, data protection, security and freedom of victims. The ethical considerations that influence individuals involved in the disaster including the survivors and the rescue team may go unrecognized within the complex situation created by the disaster.

According to the article by Dowling Jr., the European Union (EU) has a directive called the European Union Data Protection Directive which is a legislative tool that covers the privacy laws concerning individuals. The member states of the EU are required to enact its data privacy legislation in line with this directive (Dowling Jr. 2009).

4.1 Urban search and rescue (USAR)

Hew & Sunshine (2012) addresses the several deployments carried out by national USAR, coordinated by FEMA such as Oklahoma City bombing (1995), Humberto Vidal Building explosion (1996) and World Trade center (2001). These examples indicate that high buildings are constantly been targeted for artificial disaster and have more causalities when a disaster occurs.

The USAR task force includes search, rescue, technical and medical teams, each team perform their own responsibilities. Various technologies are used to locate and rescue the trapped people. This article indicates that various old techniques such as visual inspection, three points hailing, tapping on deep metal structures, highly trained search dogs are used for detecting the trapped victims. The rescue team uses portable, powerful equipment to cut, drill, lift and move heavy pieces of entangled metal and concrete. Technical and medical teams consists professionals from their fields. Each member completes the training course that makes them knowledgeable in their area as well as work together as a team.

Furthermore, it discusses about the different kinds of building collapses and the threat for both victims and rescuers within the rubble. It also explores about the features and challenges of medical teams that provides service to the victims. Additionally, it does not focus on any current technologies that are used to locate the trapped people and rescue them. (Hew & Sunshine 2002)

Kahsai & Kare (2002) indicates that when disasters occur, it is imperative that information to be released to the public should be doctored in other to avoid panic. Communication errors

are usually common during these times and can hamper the progress of a rescue operation. Also, disaster victims are usually categorized mainly using color codes to differentiate their current conditions or predicament. These colors include red which indicates victims who need immediate attention or would die otherwise, yellow which indicates victims who could wait for a further 60 minutes maximum for attention, green which indicates victims whose injuries are not life-threatening and black which means that the victims are dead.

Donnelly (2010) mentions the two categories of equipment used in building collapse rescue operations, physical search and technical search. It focuses on technical equipment such as life detector listening system and search cameras used by urban search and rescue. Life detector listening system detects the sound from the victims and also locates the source of the sound enabling rescuers to begin their rescue mission. Search cameras locate the victim and assess the victim condition. These cameras have audio capability, thermal and video capabilities and a fiber-optic scope.

According to this study, second generation locator which is a sensor network combination of a first responder unit, a stand-alone monitoring network and a command and control center has been developed to assist in urban search and rescue operations. Also, each part is tailored for a specific function in other to save lives of victims. The second generation locator has optical sensors, surveillance cameras and image processing algorithms which gives alert signals once a victim has been found. This device is also capable of sensing body heat signals, signs of life and the possibility of a hazard occurring. (Mäyrää, Känsälää, Ojalaa, Aittaa, Hietavalkamaa, Fernandezb, Hildebrandc, & Bussion 2013)

Meanwhile, there was no mention of how to secure the data collected using the second generation locator. Local radio-based short range and high power long range communication are the two ways by which communication is transmitted in the prototype locator and it is not stated how safe these means of communication are.

4.2 Data protection and privacy

McCullagh (2009) shows that existing data protection laws are obsolete and need to be revised. Also, it examines the correlation between data protection and privacy. It also states that the terms personal data, private and privacy are interpreted differently by different people because the Data Protection Directive only states these terms as a general principle.

de Herta, Papakonstantinoua, Wright & Gutwirth (2012) examines the draft proposals by the European Commission to replace the Data Protection Directive. It states that these draft proposals, General Data Protection Regulation will replace the Data Protection Directive and Po-

lice and Criminal Justice Data Protection Directive will replace a particular ethical issue which considers the processing of data in the 2008 Framework Decision.

Victor (2013) states that a regulation has been approved by the European Commission which requires that data collected about individuals and are kept even after processing such data is deleted at any time of the individual's request. Also, if such data has been shared, they should be erased as well. This means that data collected on individuals are widely protected.

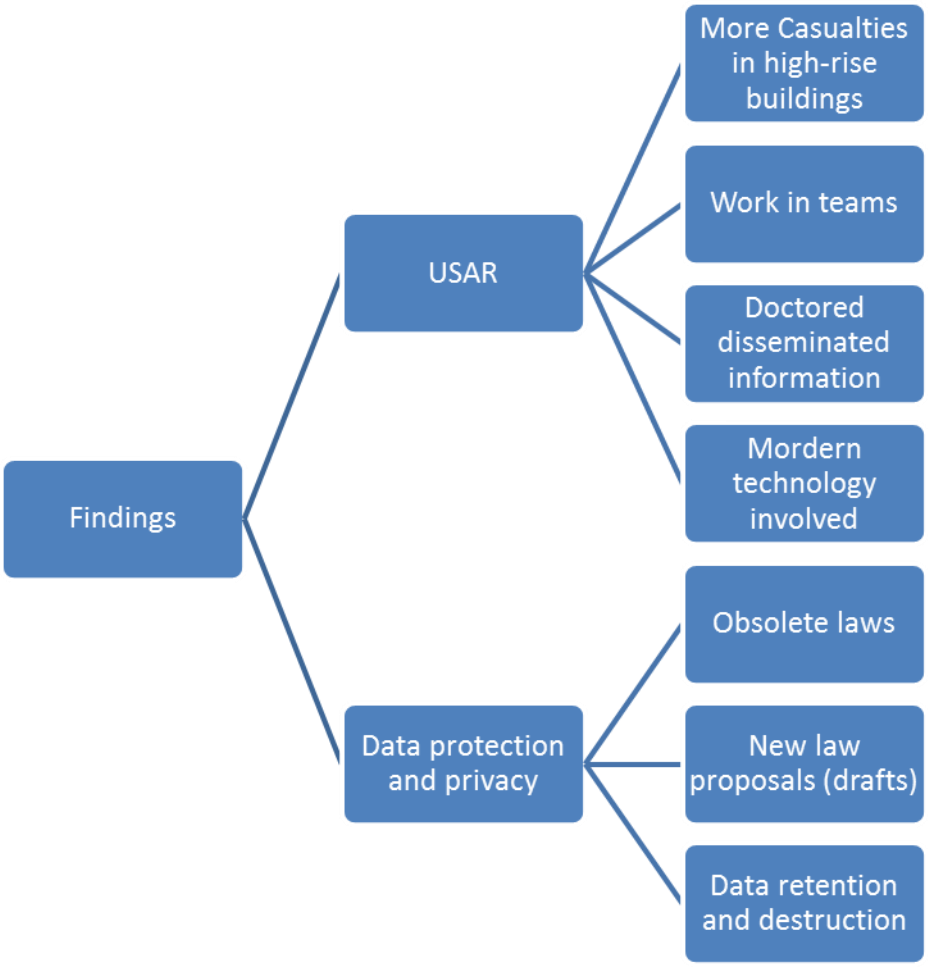

Figure 4: Findings from selected articles.

5 Discussion

There are laws in place to safeguard the privacy of individuals but all the studies about data protection and privacy indicates that new laws need to be enacted to cover for the lapses or gaps in the existing laws. According to de Herta et al. (2013), the European Commission has taken steps to create draft proposals to replace the obsolescent directive to further increase the security of individual privacy and data protection.

Donnelly (2010) and Mäyräa et al. (2013) explains how data are collected during a disaster and these data collected from the disaster site should be relayed back to the control center on ground which controls how the rescue operation is executed. These data can be physically secured by restricting access to the data storage centers and access control mechanism such as identity pass and access cards should be implemented as mentioned in 2.6.2 above. Victor (2013) discusses how data should be handled and how long it should be kept. A plan on how to store or destroy data gathered during the disaster should be made so as to protect the victim's personal information. If data is to be stored, those who intend to keep the information should seek the approval of information owners and if data is to be destroyed, a proper destruction plan should be in place and executed at a predetermined time.

McCullagh (2009) and de Herta et al. (2012) explains how laws guiding data protection and privacy are obsolescent and need to be updated to further protect victims. Laws and mechanisms which can protect information of victims should be implemented for rescue operations. The use of virtual private networks (VPN) serves as a protection mechanism by which data and privacy of victims can be secured. Cheung and Mišić (2001) indicate that VPN will ensure the confidentiality, authenticity, integrity within the network's environment while information is passed from one end to the other.

There are certain information security standards which the USAR should consider implementing in order to ensure the protection of information and privacy in every operation. IT-Grundschutz is a security standard which would help improve the security levels of any organization. Some points above in this thesis (2.5 and 2.6) were deduced from the IT-Grundschutz. Also, standards such as those published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC) are widely known to have good frameworks which guarantee decent information security practices. These standards will help the USAR, if implemented, further guarantee that the information of victims are protected.

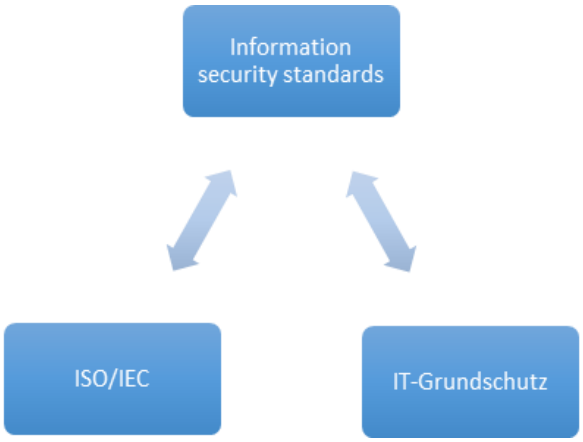

Figure 5: Examples of information security standards

5.1 Reliability and trustworthiness

This study process was carried out using the systematic literature approach and the reviewers are inexperienced in the field of systematic research but studied other systematic reviews in other to be conversant with this literature process. The article search and selection process were notably time consuming.

Limited research has been done on this subject serving as a constraint in finding the suitable articles and journals for this study. Resources for this thesis include articles that study Urban Search and Rescue, data protection and privacy. However, the inclusion and exclusion criteria showed which articles were beneficial to this research as it described what type of articles were used and why it was used. Though this review had two reviewers, it still lacks the value needed due to the fact that previous studies on some areas of this subject were unavailable. However, data was extracted from the articles available to draw a reasonable conclusion on the subject matter.

5.2 Project work and learning reflection

This project was introduced to us by our teacher who became our supervisor. He spoke to us about this project because we were interested in data protection and security issues for a thesis project. We perceived this project as an opportunity to be part of something big and it was a way of contributing to the European Union development as a whole.

We were able to take advantage of what we were taught in class, for example, time management, creating deadlines and meeting up to the set deadlines and apply them during this project work. They proved very useful in every way. Even though we had some experience in setting targets, this project work gave us a better insight of a proper project-based environment with high importance. Practicing the act of confidentiality was also a welcomed experience. The art of searching for credible resources was another area in which we gained more experience during this project even though it took a lot of time and patience but it is seen as knowledge added on our part.

Due to the fact that this project was part of a whole project, there was limited time to do all that was necessary considering the insufficient or unavailability of materials and resources needed. We believe that if all the resources needed for this thesis were readily available, better results would have been achieved.

5.3 Conclusion

This study shows that various means are explored by urban search and rescue during the occurrence of a disaster including man, animal and technology to rescue victims and management of such disaster. Rescue missions are evolving, technology is more involved in rescue missions now than ever before and new technologies will continue to be developed for increased success in rescue missions as well as to minimize risks.

Victim's general information such as name, job status, address, etc. become available to USAR operatives and also, personal information such as social security number and family details are secured to help further the rescue mission. Families of the victims deserve to get updates concerning any member involved in the disaster. USAR operatives also acquire information about victims and their environment by accessing feeds from cameras installed at certain spots within the environment. Calls from eye witnesses to call centers also serve as a means of collecting data about disasters and is helpful in gaining knowledge about situations. These information help the USAR team in carrying out rescue missions successfully.

Irrespective of whether individuals are walking free or within the rubbles of a disaster, data protection and privacy laws apply equally to everyone and should be taken seriously. Negligence to protect or secure the data of victims should be classified as a breach on privacy of individuals and punishable as such. Data of identifiable individuals need to be protected and secured irrespective of where it has been gathered.

5.4 Recommendations

Due to the fact that research articles could not be found relating to how the data collected about search and rescue victims are used and protected, it is recommended that future studies should be carried out into this area of interest.

USAR teams from different countries are guided by standards and legislations enacted by their country to ensure the privacy for example, in United States, federal privacy act and the health insurance portability act (HIPAA) are leading legislation regarding privacy and USAR teams in United States are entitled to follow them. It is our advice that when future studies are initiated, interviews to USAR operatives or first responders should serve an important means of data collection.

References

Britz, M. 2013. Computer forensics and cyber crime: an introduction. Boston: Pearson.

Bundesamt für Sicherheit in der Informationstechnik. 2005. IT-Grundschutz catalogues. Accessed 17 November 2014 https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/it-grundschutz-kataloge_2005_pdf_en_zip.zip?__blob=publicationFile

Cheung, K.H. Mišić, J. 2002. On virtual private networks security design issues. Computer Networks. Volume 38, Issue 2, Pages 165-179. Accessed 19 May 2015.

Clarke, R. 2013. Introduction to Dataveillance and Information Privacy, and Definitions of Terms. Accessed 6 February 2015. http://www.rogerclarke.com/DV/Intro.html#Priv

Computer Hackers and Predators. Webroot. Accessed 17 November 2014 http://www.webroot.com/us/en/home/resources/articles/pc-security/computer-security-threats-hackers

Common Mistakes When Destroying Data Yourself. 2013. West Coast Computer Recycler. 30 August. Accessed 17 November 2014 http://www.wcrecycler.com/blog.php?headline=Common%20Mistakes%20When%20Destroying%20Data%20Yourself&id=1227

Data Protection and Breach Readiness Guide. 2014. Online Trust Alliance. Accessed 2 December 2014. https://otalliance.org/system/files/files/best-practices/documents/2014otadatabreachguide4.pdf

de Hert, P. Papakonstantinou, V. Wright, D. & Gutwirth, S. 2013. The proposed regulation and the construction of a principles-driven system for individual data protection, Innovation: The European Journal Of Social Sciences, 26, 1/2, pp. 133-144, Academic Search Elite, EBSCOhost, viewed 10 December 2014.

Donnelly, T. 2010. Building Collapse Rescue Operations: Technical Search Capabilities, Fire Engineering, 163, 10, pp. 22-26, Academic Search Elite, EBSCOhost, viewed 10 December 2014.

Dowling Jr., D. C. 2009. International Data Protection and Privacy Law. White & case, August. Accessed 27 November 2014 http://www.whitecase.com/files/publication/367982f8-6dc9-478e-ab2f-5fdf2d96f84a/presentation/publicationattachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_intldataprotectionandprivacylaw_v5.pdf

Employment Background Checks: A Jobseeker's Guide. 1994. Revised 2014. Accessed 25 November 2014 https://www.privacyrights.org/employment-background-checks-jobseekers-guide

European Union Agency for Fundamental Rights and Council of Europe. 2014. Handbook on European data protection law, April. Accessed 27 November 2014 http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf

Five IT Disposal Mistakes Not to Make. 2014. Retire-IT, Accessed 17 November 2014 http://retire-it.com/wp-content/uploads/2014/01/Retire-IT-Five-Mistakes-Not-To-Make.pdf

Gregg, M. 2013. Certified ethical hacker (CEH) cert guide. Indianapolis, IN: Pearson IT Certification

Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). 2010. National Institute of Standards and Technology. Accessed 2 December 2014.
http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

Guidance Document: Taking Privacy into Account Before Making Contracting Decisions. 2010. Accessed 7 December 2014.
http://www.tbs-sct.gc.ca/atip-aiprp/tpa-pcp/tpa-pcp06-eng.asp

Herold, R. 2006. Addressing Privacy Issues During Disaster Recovery. Accessed 2 December 2014.
http://www.dis.arkansas.gov/security/Documents/Herold.pdf

Hew, P, & Sunshine, W. 2002. Urban search and rescue, Topics In Emergency Medicine, 24, 3, pp. 26-36, CINAHL with Full Text, EBSCOhost, viewed 10 December 2014.

Horwath, J. 2012. Setting Up a Database Security Logging and Monitoring Program. Accessed 7 December 2014.
http://www.sans.org/reading-room/whitepapers/application/setting-database-security-logging-monitoring-program-34222

Janes, P. 2012. People, Process, and Technologies Impact on Information Data Loss. Accessed 7 December 2014.
http://www.sans.org/reading-room/whitepapers/dlp/people-process-technologies-impact-information-data-loss-34032

Kahsai, D. & Kare, J. 2002. Prehospital disaster management: implications for weapons of mass destruction, Topics in Emergency Medicine, 24, 3, pp. 37-43, CINAHL with Full Text, EBSCOhost, viewed 10 December 2014.

Kotler,J. 2009. User-centric privacy. Lohmar: JOSEF EUL VERLAG GmbH.

McCullagh, K. 2009. Protecting 'privacy' through control of 'personal' data processing: A flawed approach, International Review of Law, Computers & Technology, 23, 1/2, pp. 13-24, Academic Search Elite, EBSCOhost, viewed 10 December 2014.

Mäyrä, A. Känsälä. K, Ojala, K. Aitta, P. Hietavalkama, T. Fernandez, F. Hildebrand, L. & Bussion, J. 2013. Optical Sensors and Algorithms for Life-Sign Detection in USaR-Operations, AIP Conference Proceedings, 1537, 1, pp. 41-46, Academic Search Elite, EBSCOhost, viewed 10 December 2014.

Physical and environmental security. 2008. University of Miami Leonard M. Miller School of Medicine. Accessed 2 December 2014.
http://it.med.miami.edu/x2230.xml

Sloan, R. & Warner, R. 2014. Unauthorized access: the crisis in online privacy and security Boca Raton, FL.

Stutzman, K. 2012. Data Destruction – Protecting private data when moving to or from a cloud service. Ongoing operations. Accessed 25 November 2014
http://ongoingoperations.com/blog/2012/12/data-destruction-protecting-private-data-cloud-service/

The Universal Declaration of Human Rights. 2015. Accessed 6 February 2015.
http://www.un.org/en/documents/udhr/

Three Common Information Disposal Mistakes and How You Can Prevent Them. Archives Management Centers, Inc., 12 February. Accessed 17 November 2014
http://www.archives-amc.com/three-common-information-disposal-mistakes-can-prevent/

Top Data Security Mistakes Most Companies Make. 2013. Datashield, 23 October. Accessed 17 November 2014
http://datashieldcorp.com/2013/10/23/top-data-security-mistakes-companies-make/

Victor, J.M. 2013, The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy, Yale Law Journal, 123, 2, pp. 513-528, Academic Search Elite, EBSCOhost, viewed 10 December 2014.

Violino, B. 2012. The in-depth guide to data destruction. CSO online. 6 February. Accessed 25 November 2014
http://www.csoonline.com/article/2130822/it-audit/the-in-depth-guide-to-data-destruction.html

Wong, J & Robinson, C. 2004. Urban Search and Rescue Technology Needs: Identification of Needs: Identification Of Needs. Accessed 5 February 2015.
https://www.ncjrs.gov/pdffiles1/nij/grants/207771.pdf

Figures

Figure 1: Common issues with data protection and privacy..... 14
Figure 2: Solutions to common issues with data protection and privacy 19
Figure 3: The literature review process. 21
Figure 4: Findings from selected articles. 24
Figure 5: Examples of information security standards 25

Tables

Table 1: depicts the literature search results and the categorized number of hits using five different keywords. 20
Table 2: This table shows the inclusion and exclusion criteria. 20